IP 주소관리를 통한 네트워크 차단

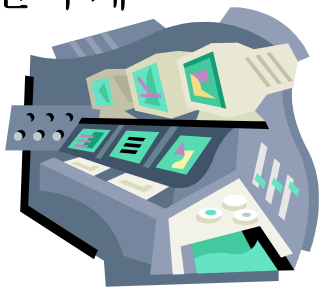
2005. 11. 25.

발 표 자 : 김 현철 (ICU)

목 차

I. IP 주소관리의 필요성

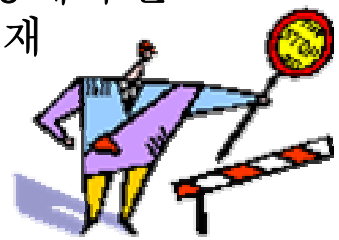
인가된 IP 주소에 대한 사용/미사용 모니터링 수단 부재



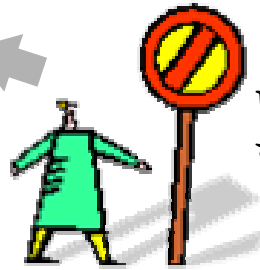
네트워크 자원의 수동관리로 인한 인적 자원 낭비 및 업무 능률 저하

내부 사용자의 IP 도용에 따른 장애 및 내부 보안 문제 발생

비인가 IP 주소에 대한 사용 통제 수단 부재



네트워크 주소 인증을 통한 정책 기반 실시간 네트워크 차단/통제 시스템이 필요



미 할당 IP에 대한 접근 통제 부재

실시간 IP 자원 파악 및 증설 결정 시 근거 자료 부재

IP 주소관리 시스템의 목표

목적: 네트워크 주소(IP/MAC) 인증을 통한 정책 기반 실시간 네트워크 차단/통제 시스템

관리 기능	제어 기능	보고서 기능
◆ 네트워크 주소 자동 수집 ◆ 미사용/사용 IP 정보 제공 ◆ 충돌 정보 제공 ◆ 장애에 대한 보고서 기능 ◆ 시스템 정보 제공 기능 ◆ 인증 IP에 대한 보호	◆ IP 사용에 대한 투명성 확보 ◆ IP 충돌로 인한 장애 제거 ◆ 비인가 IP에 대한 차단 ◆ 비인가 MAC에 대한 차단	◆ IP별 변경 로그 관리 ◆ MAC별 변경 로그 관리 ◆ 이벤트 로그 제공 ◆ IP 관련 장애에 대한 보고서

IP 주소관리를 위한 ARP

- ARP: TCP/IP 네트워크에서 논리적 주소인 IP 주소를 물리적 주소인 하드웨어 주소로 대응시키기 위해 사용되는 프로토콜

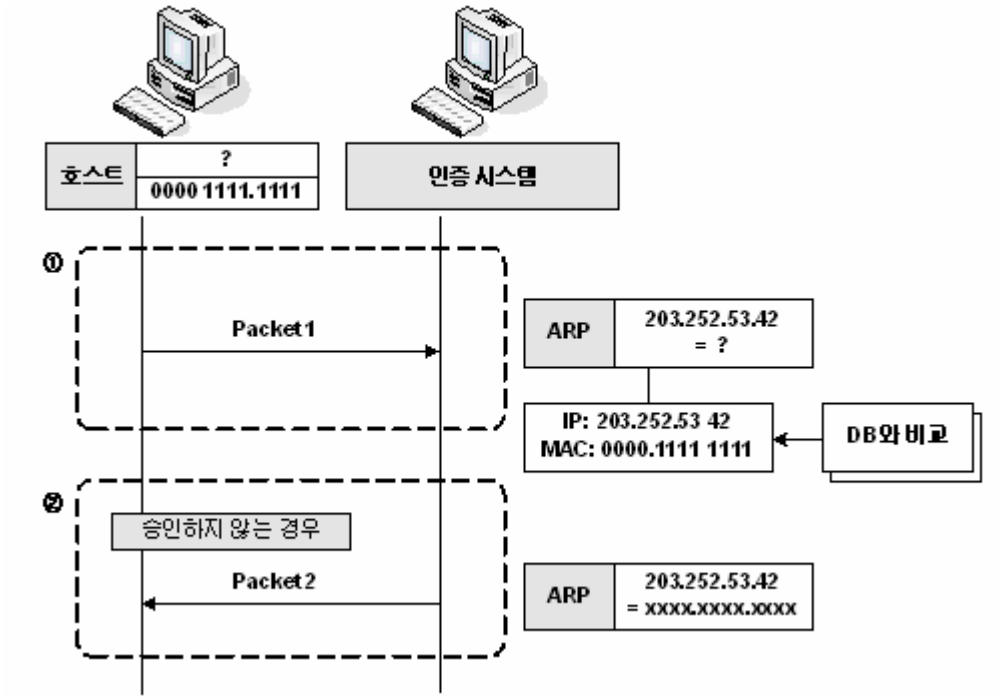
- ARP로 수집된 IP 주소와 물리적 네트워크 주소 정보는 ARP 캐시라 불리는 메모리에 테이블 형태로 저장됨

- Gratuitous ARP: 컴퓨터가 최초 부팅 될 때 주로 사용되며 어떤 호스트가 자신의 IP 주소가 사용 중인지 판별하는 용도로 사용

네트워크 설정의 변경 없이 IP 주소 인증 시스템 구축 가능

IP 주소 인증 메커니즘

ARP를 이용하면 브로드캐스트 범위 내 전체 네트워크의 IP주소 인증 가능



호스트가 IP 주소를 사용하기 시작할 때 Gratuitous ARP 메시지 브로드캐스팅

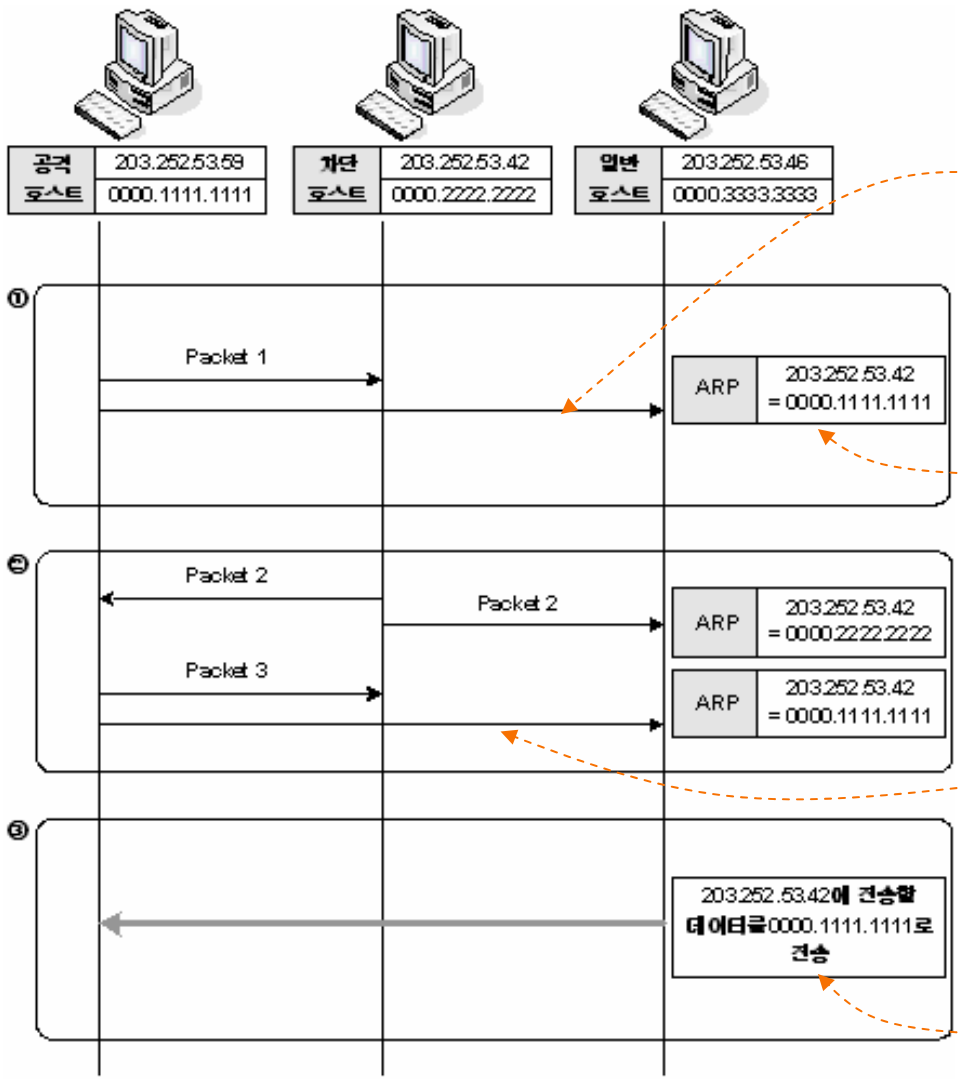
인증 시스템이 호스트가 보낸 Gratuitous ARP 패킷을 받아 IP 주소와 MAC 주소를 분석하여 적절한 사용인지 비교

허가 시
동작 없음.

불허가 시
②번과 같이 자신이 해당 IP 주소를 사용하고 있음을 ARP 응답 메시지를 통해 전송

IP 스푸핑

ARP 스푸핑: ARP 패킷의 MAC 주소를 속여 특정 호스트의 패킷을 가로채는 방법



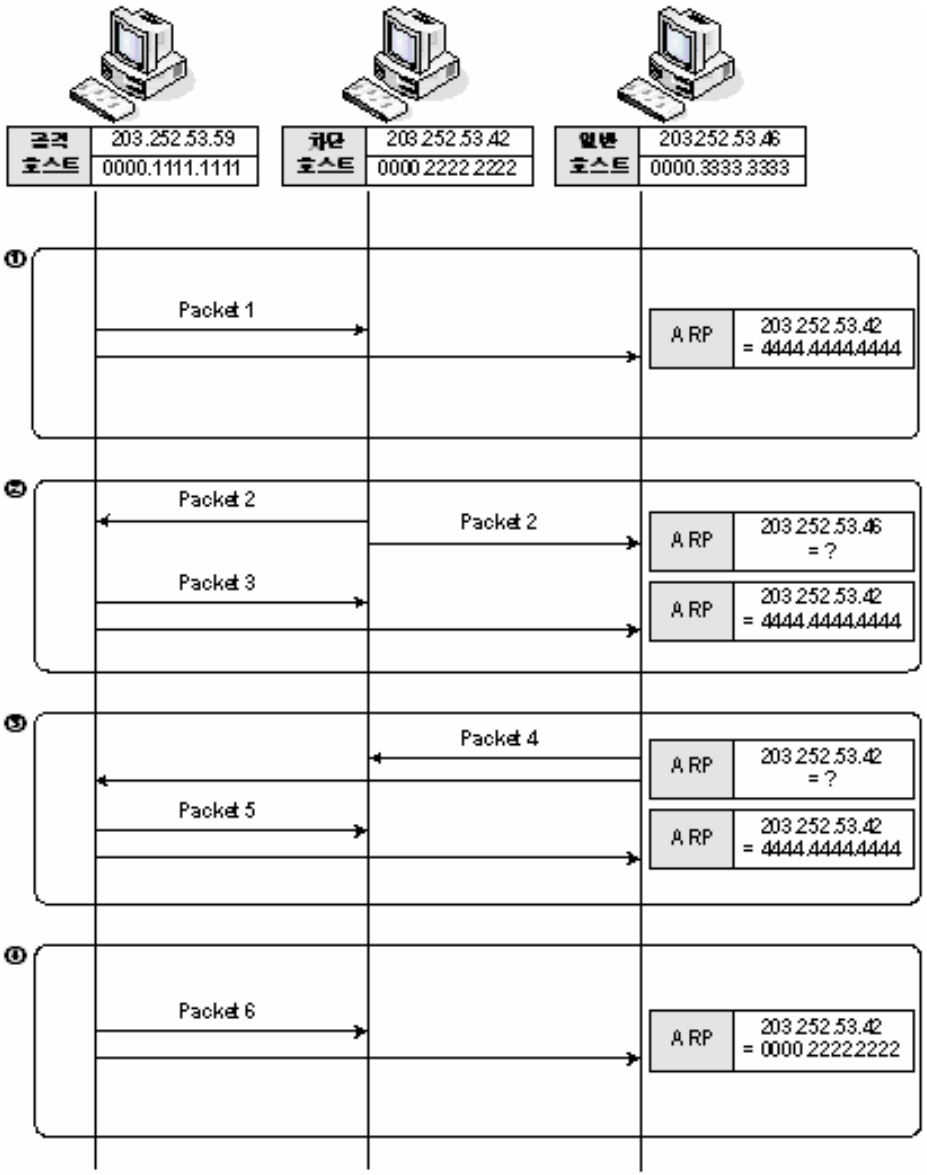
공격 호스트가 일반 호스트에게 수집하려는 호스트의 IP 주소에 자신의 MAC 주소를 매치 시켜 브로드캐스팅

공격 호스트가 보낸 패킷을 받은 일반 호스트는 자신의 ARP 캐시 테이블을 업데이트

피해 호스트가 올바른 MAC 주소가 담긴 패킷을 보내면 공격 호스트는 다시 틀린 MAC 주소의 패킷을 보내어 일반 호스트의 ARP 캐시 테이블을 업데이트 시킴.

공격 호스트는 피해 호스트로 갈 패킷을 가로챌 수 있음.

ARP 차단 메커니즘 – ARP 스푸핑

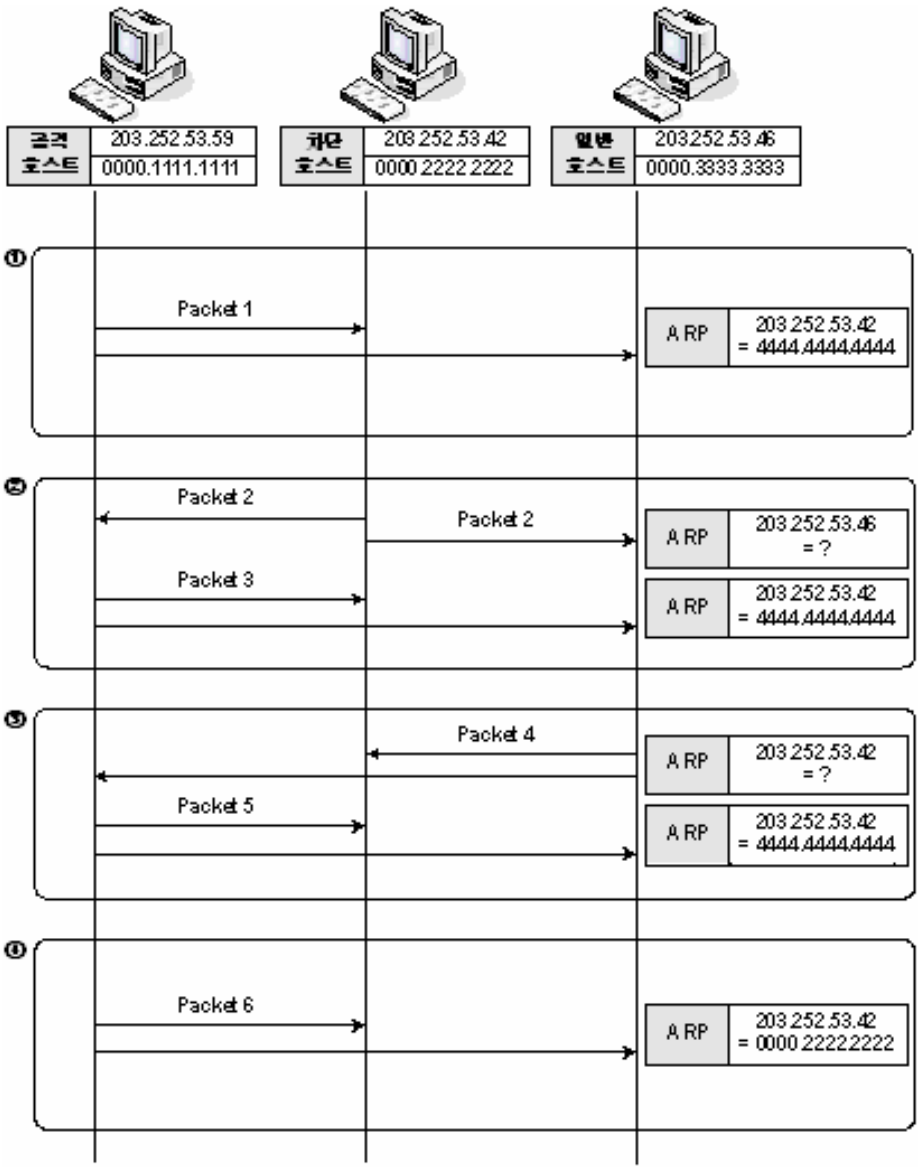


① 차단 호스트의 차단: Packet1에 차단 호스트의 잘못된 MAC정보를 담아 전송. 일반 호스트는 그에 따라 ARP 캐시 테이블 업데이트

② 차단 호스트가 일반 호스트와 통신하기 위하여 Packet2를 전송. Packet2를 받은 공격 호스트는 잘못된 MAC 정보가 있는 Packet3를 보냄.

③ 일반 호스트가 차단 호스트와 통신하기 위하여 Packet4를 전송. Packet4를 받은 공격 호스트는 잘못된 MAC 정보가 있는 Packet5를 보냄.

ARP 차단 메커니즘 – ARP 스푸핑



④ 차단 호스트의 해제: Packet4에 차단 호스트의 올바른 MAC 정보를 담아 전송. 일반 호스트는 그에 따라 ARP 캐시 테이블 업데이트

3. OS별 Gratuitous ARP 동작

- Gratuitous ARP는 OS마다 ARP 패킷 내의 필드 값과 확인하는 횟수가 설정 값에 따라 다름.
- DN (Defending Node): 이미 IP를 할당 받고 사용하는 호스트
- ON (Offending Node): 이미 사용 중인 IP를 사용하려고 시도하는 호스트

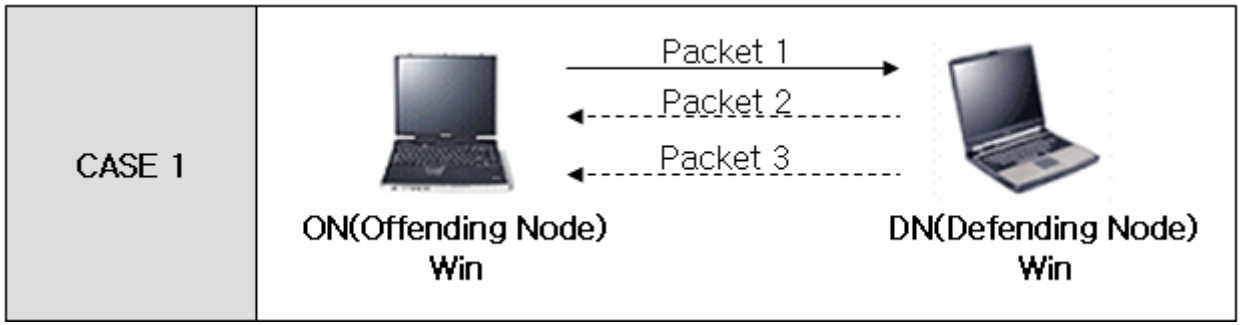
- Windows: 2003, XP Version
- Linux: Red Hat 7.2, Wow 7.3
- A: Defending Node (이미 할당된 IP를 사용하고 있는 사용자)
- B: Offending Node (이미 할당된 IP를 사용하려고 시도하는 다른 사용자)
- C: Others (나머지 호스트들)
- C_IP => Conflicting IP Address

OS별 Gratuitous ARP 동작

(1) Window(ON) – Window(DN)

Gratuitous ARP 반응

- C(Others)'s 캐시 테이블: DN의 MAC
- DN에 IP 충돌 메시지 표시, ON은 IP 사용할 수 없음.



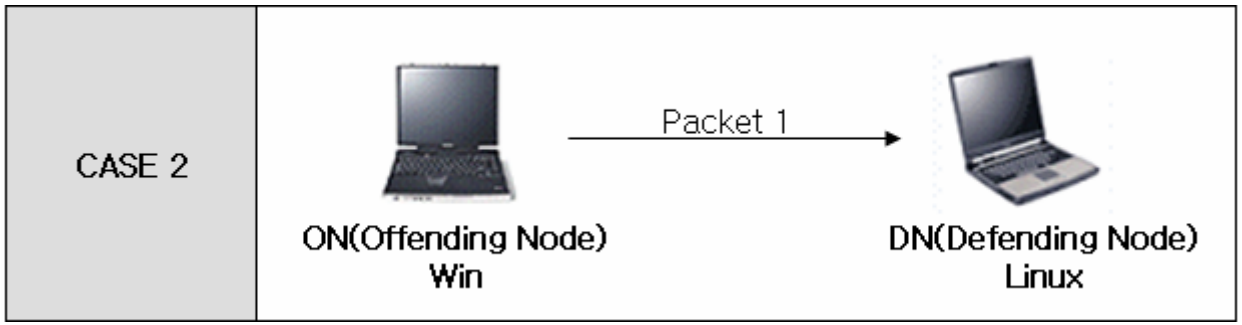
Op Type	Src	Dst	SPA	SHA	TPA	THA
Packet 1 (Request)	B.MAC	ALL	C_IP(B)	B.MAC	C_IP(B)	Ignored
Packet 2 (Response)	A.MAC	B.MAC	C_IP(A)	A.MAC	C_IP(B)	B.MAC
Packet 3 (Request)	A.MAC	ALL	C_IP(A)	A.MAC	C_IP(A)	Ignored

OS별 Gratuitous ARP 동작

(2) Window(ON) – Linux(DN)

Gratuitous ARP 반응

- C(Others)'s 캐시 테이블: 서로 경쟁적으로 캐시 테이블 갱신
- DN과 ON은 Duplicated IP를 사용



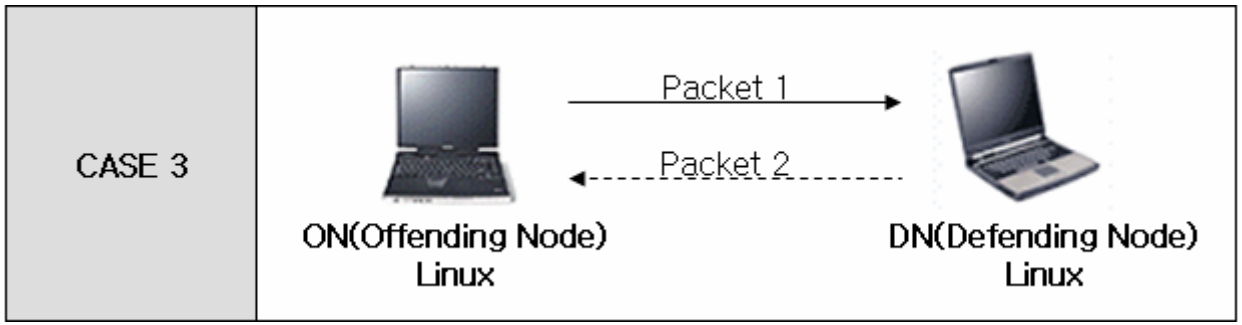
Op Type	Src	Dst	SPA	SHA	TPA	THA
Packet 1 (Request)	B.MAC	ALL	C_IP(B)	B.MAC	C_IP(B)	Ignored

OS별 Gratuitous ARP 동작

(3) Linux(ON) – Window(DN)

Gratuitous ARP 반응

- C(Others)'s 캐시 테이블: DN의 MAC
- DN에 IP 충돌 메시지 표시되지 않고, ON은 IP 사용할 수 없음.



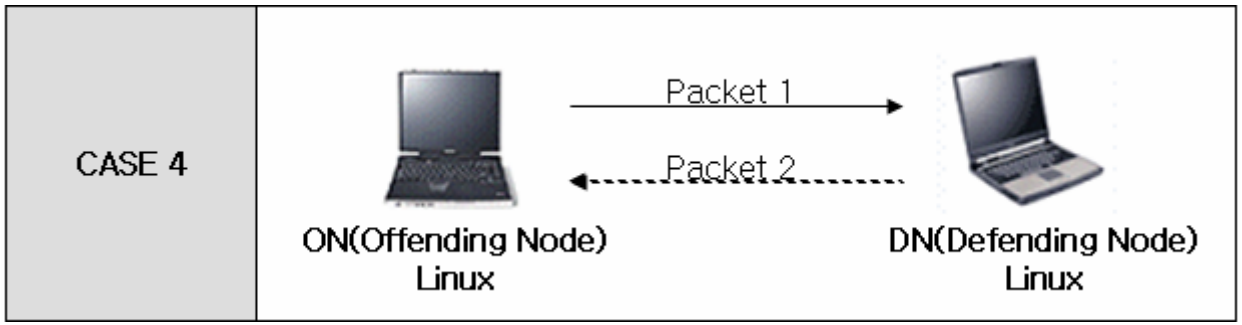
Op Type	Src	Dst	SPA	SHA	TPA	THA
Packet 1 (Request)	B.MAC	ALL	0.0.0.0	B.MAC	C_IP(B)	Ignored
Packet 2 (Response)	A.MAC	B.MAC	C_IP(A)	A.MAC	0.0.0.0	B.MAC

OS별 Gratuitous ARP 동작

(4) Linux(ON) – Linux(DN)

Gratuitous ARP 반응

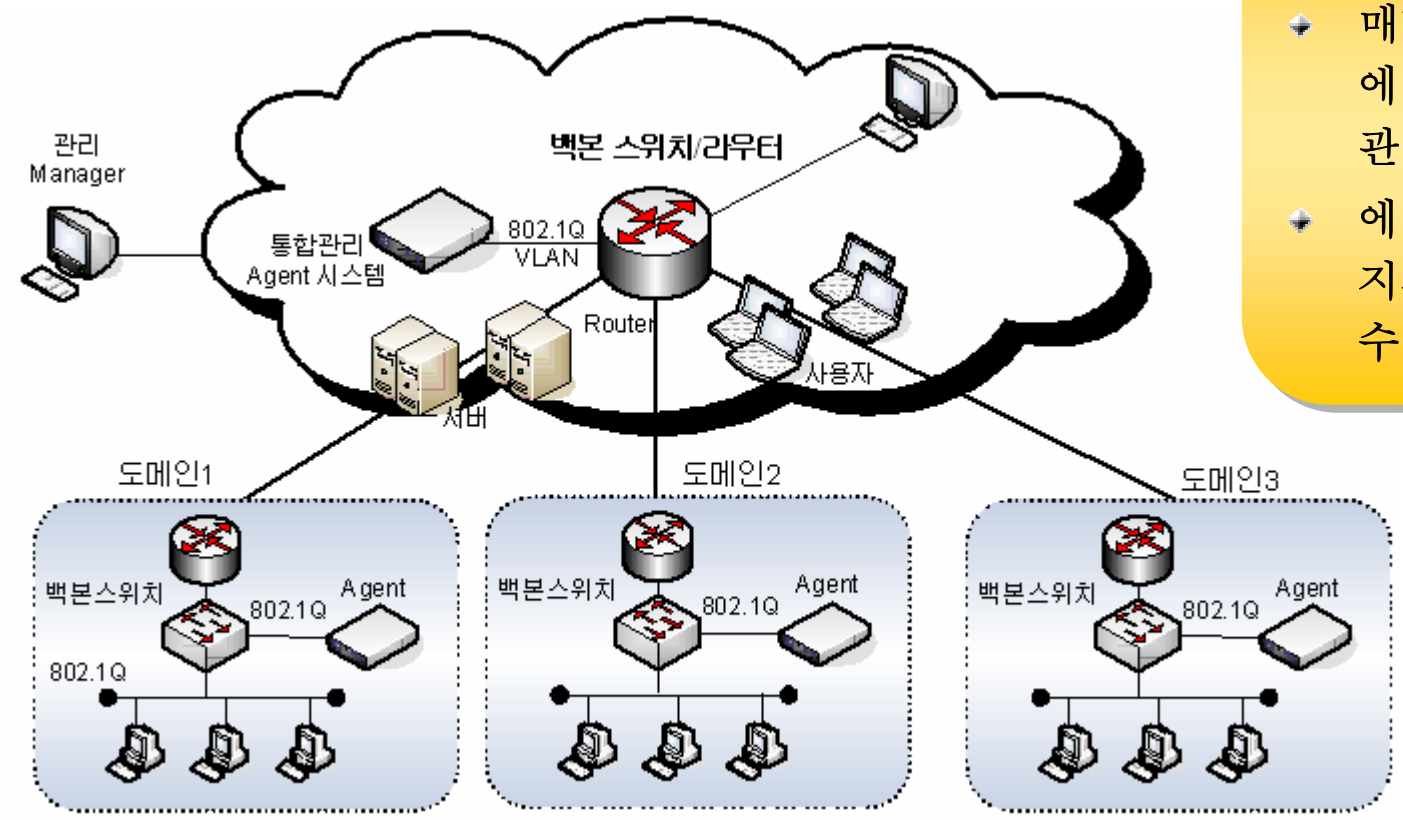
- C(Others)'s 캐시 테이블: DN의 MAC
- ON은 IP 사용할 수 없음.



Op Type	Src	Dst	SPA	SHA	TPA	THA
Packet 1 (Request)	B.MAC	ALL	0.0.0.0	B.MAC	C_IP(B)	Ignored
Packet 2 (Response)	A.MAC	B.MAC	C_IP(A)	A.MAC	C_IP(A)	B.MAC

IP 주소/차단 시스템 구조 - 1

시스템을 매니저와 에이전트로 분리



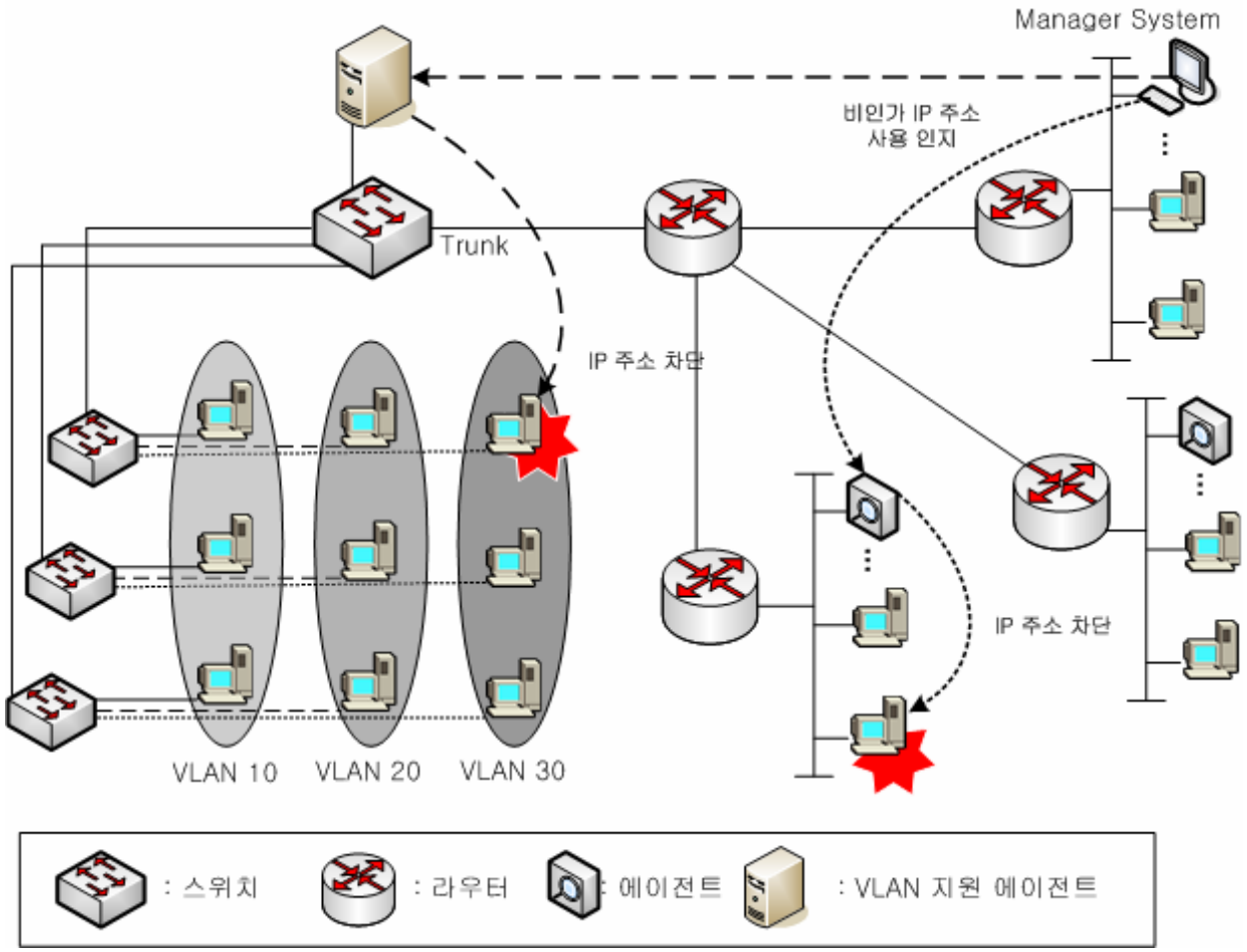
시스템 동작

- 매니저: 각 네트워크에 존재하는 에이전트 관리
- 에이전트: 매니저가 지시하는 관리 정책들 수행

IP 주소/차단 시스템 구성

매니저	OS: Window 기반의 운영체제 Tool: Visual Basic 6.0 Crystal Report Install Shied 6.0 Database: Microsoft Access
에이전트	OS: Linux 7.3/9.0 Tool: C Language Compile: gcc Capture Tool: pcap library Database: Shared Memory

IP 주소/차단 시스템 구성 - 2



<비인가 IP 주소 사용 인지 테스트베드>

IP 주소/차단 시스템 구성 - Policy

IP 차단

IP 차단으로 설정된 IP는 통신을 할 수 없도록 차단됨.
차단된 IP로는 통신 할 수 없음.

4		192.168.2.4	00:00:00:00:00:00	None						
5		192.168.2.5	00:02:B3:B4:2B:4F	Unknown						U/Linux
6		192.168.2.6	00:02:B3:B4:30:3A	PC010						WIN
7		192.168.2.7	00:02:B3:B4:2A:11	PC011						WIN
8		192.168.2.8	00:02:B3:B4:2B:4E	PC012		IP 차단				WIN
9		192.168.2.9	00:00:00:00:00:00	None						
10		192.168.2.10	00:00:00:00:00:00	None						
11		192.168.2.11	00:00:00:00:00:00	None						
12		192.168.2.12	00:00:00:00:00:00	None						
13		192.168.2.13	00:00:00:00:00:00	None						
14		192.168.2.14	00:00:00:00:00:00	None						
15		192.168.2.15	00:00:00:00:00:00	None						

IP 주소/차단 시스템 구성 - Policy

MAC 차단

MAC 차단으로 설정된 MAC은 통신을 할 수 없도록 차단됨. 즉 차단된 랜 카드를 다른 호스트에 설치하여도 통신 할 수 없음. (현재 사용 중인 MAC에만 가능)

4		192.168.2.4	00:00:00:00:00:00	None						
5		192.168.2.5	00:02:B3:B4:2B:4F	Unknown						U/Linux
6		192.168.2.6	00:02:B3:B4:30:3A	PC010						WIN
7		192.168.2.7	00:02:B3:B4:2A:11	PC011		MAC 차단				WIN
8		192.168.2.8	00:02:B3:B4:2B:4E	PC012						WIN
9		192.168.2.9	00:00:00:00:00:00	None						
10		192.168.2.10	00:00:00:00:00:00	None						
11		192.168.2.11	00:00:00:00:00:00	None						
12		192.168.2.12	00:00:00:00:00:00	None						
13		192.168.2.13	00:00:00:00:00:00	None						
14		192.168.2.14	00:00:00:00:00:00	None						
15		192.168.2.15	00:00:00:00:00:00	None						

IP 주소/차단 시스템 구성 - Policy

IP 고정

IP 고정으로 설정된 IP는 그 MAC에서만 통신 가능하지만 그 MAC은 다른 IP 사용 가능.
IP를 보호하는 차원에서 서버나 통신장비 등과 같은 중요 IP와 충돌되는 것을 막기 위한 것 (IP 변경이 없는 서버나 통신장비를 위주로 사용)

4		192.168.2.4	00:00:00:00:00:00	None						
5		192.168.2.5	00:02:B3:B4:2B:4F	Unknown						U/Linux
6		192.168.2.6	00:02:B3:B4:30:3A	PC010		IP 고정				WIN
7		192.168.2.7	00:02:B3:B4:2A:11	PC011						WIN
8		192.168.2.8	00:02:B3:B4:2B:4E	PC012						WIN
9		192.168.2.9	00:00:00:00:00:00	None						
10		192.168.2.10	00:00:00:00:00:00	None						
11		192.168.2.11	00:00:00:00:00:00	None						
12		192.168.2.12	00:00:00:00:00:00	None						
13		192.168.2.13	00:00:00:00:00:00	None						
14		192.168.2.14	00:00:00:00:00:00	None						

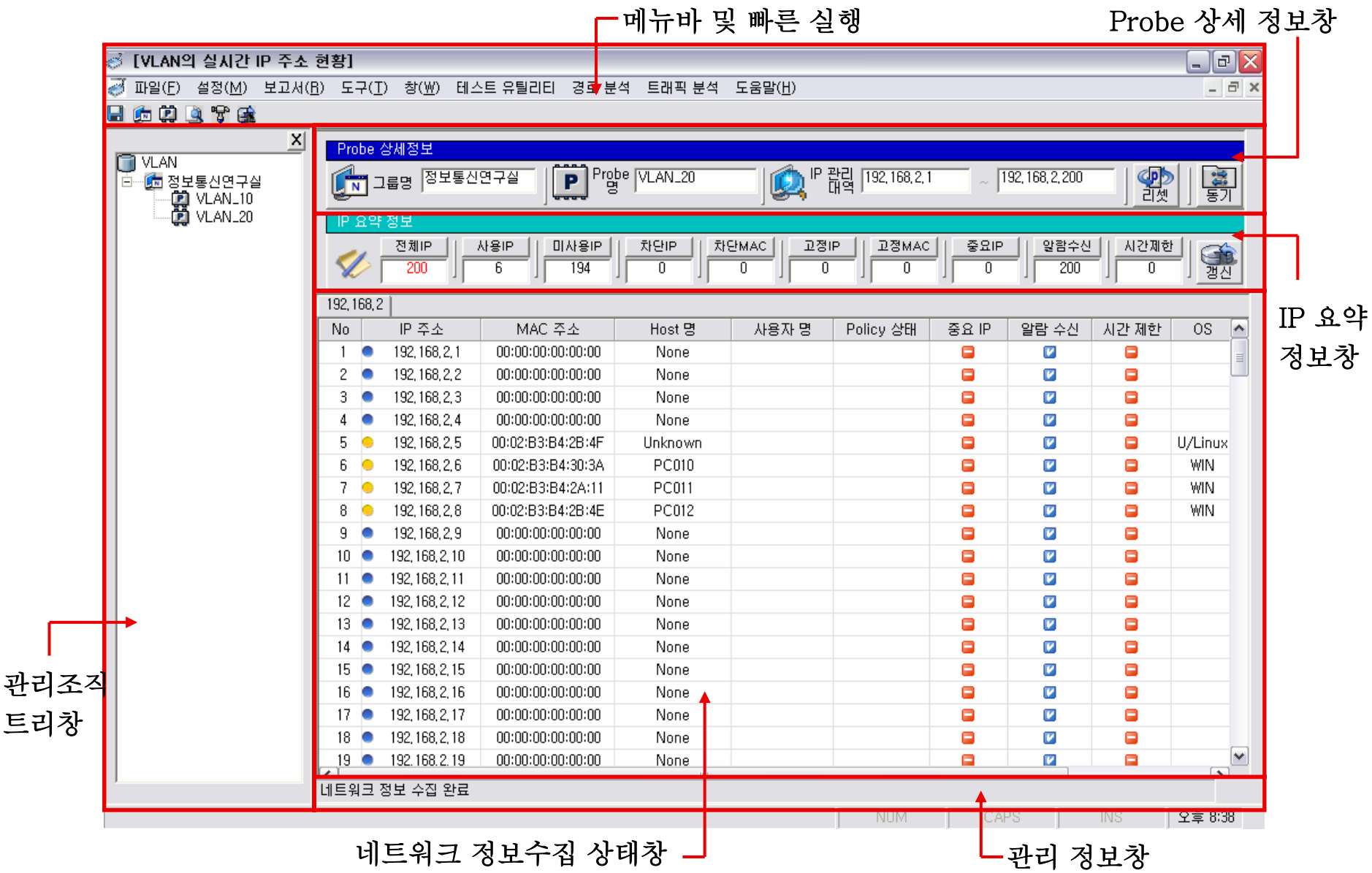
IP 주소/차단 시스템 구성 - Policy

MAC 고정

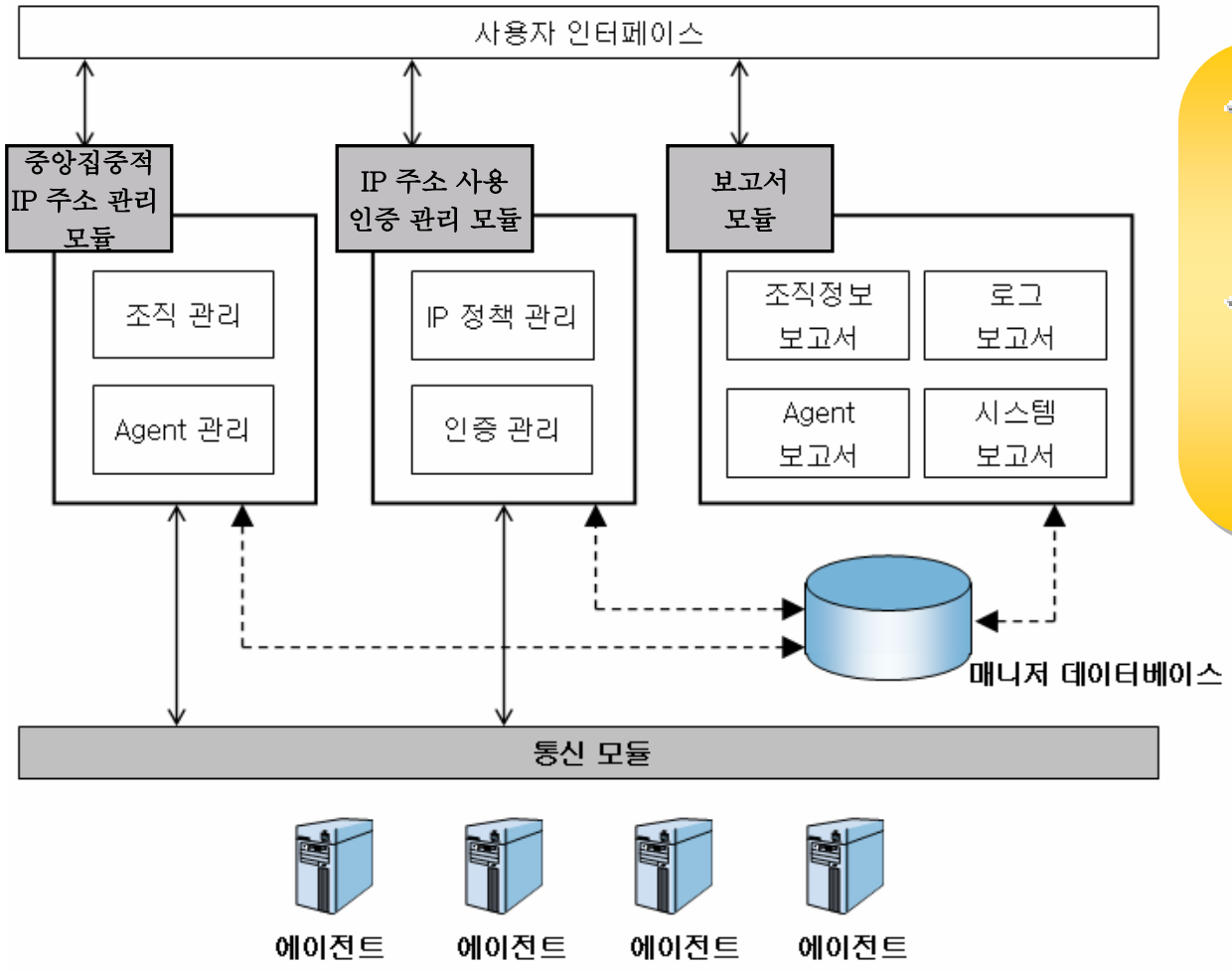
MAC 고정으로 설정된 MAC은 그 IP에서만 통신 할 수 있지만 그 IP는 다른 MAC에서 사용 가능.
사용자들은 자신의 PC에서 IP를 바꿔가며 사용하는 것을 막고자 할 경우 사용.

4		192.168.2.4	00:00:00:00:00:00	None						
5		192.168.2.5	00:02:B3:B4:2B:4F	Unknown		MAC 고정				U/Linux
6		192.168.2.6	00:02:B3:B4:30:3A	PC010						WIN
7		192.168.2.7	00:02:B3:B4:2A:11	PC011						WIN
8		192.168.2.8	00:02:B3:B4:2B:4E	PC012						WIN
9		192.168.2.9	00:00:00:00:00:00	None						
10		192.168.2.10	00:00:00:00:00:00	None						
11		192.168.2.11	00:00:00:00:00:00	None						
12		192.168.2.12	00:00:00:00:00:00	None						
13		192.168.2.13	00:00:00:00:00:00	None						
14		192.168.2.14	00:00:00:00:00:00	None						

Manager System - 1



Manager System - 2



- 각 모듈은 매니저의 기능을 중심으로 모듈화 되어 있음.
- 중앙집중적 IP 주소 관리 모듈, IP 주소 사용 인증 관리 모듈, 보고서 모듈로 구성

Manager System - 3

- 현재 네트워크에서 사용되는 IP 주소 현황을 모니터링 하는 기능 제공
- 실시간 IP 주소 사용 현황 확인
- 비 인가된 사용자에 대해 IP 주소를 차단

(1) 중앙집중적 IP 주소 관리 기능

에이전트 시스템들이 수집한 네트워크 정보 및 IP 주소를 수신하여 중앙에서 관리

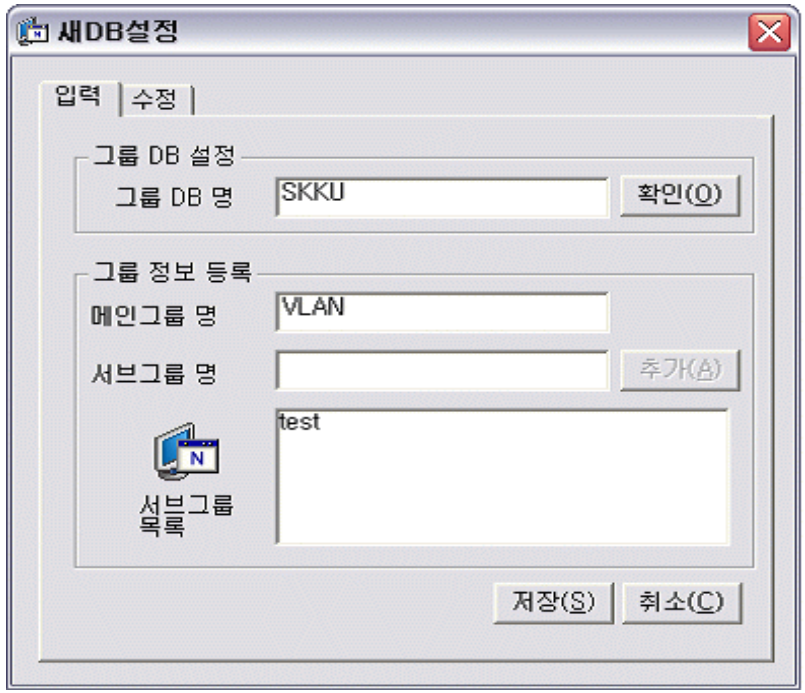
- IP 주소의 중복 사용을 피할 수 있음.
- 전체적인 IP 주소 사용 내역을 통계 낼 수 있음.

(1) 중앙집중적 IP 주소 관리 기능

그룹 등록 관리

IP 주소별, 부서별, 층별로 사용자 그룹을 설정

- 실제 IP 주소 사용 여부 확인
- 고정 IP 주소 및 MAC 주소에 대한 그룹별 사용 내역 관리



상세 정보 관리

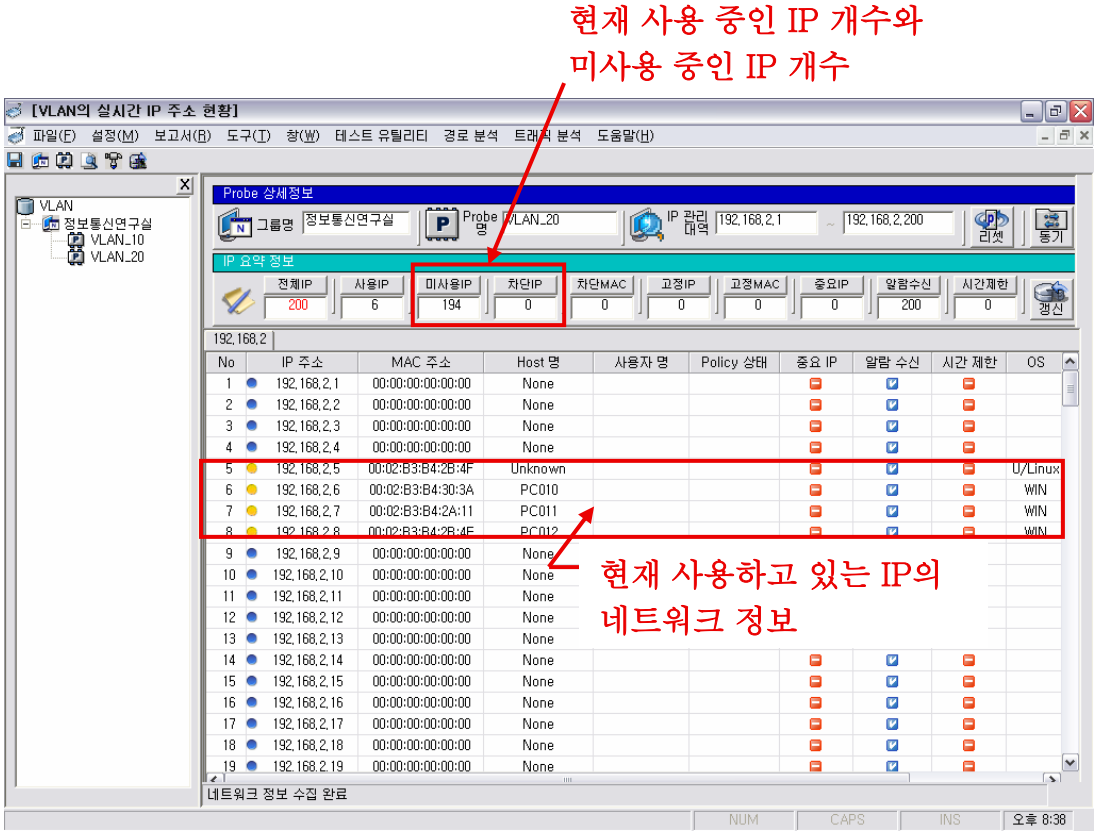
사용자 관리 목록을 통하여 특정 사용자나 장비에 대한 상세 정보 및 중요한 사항을 기록하여 관리

(2) IP 주소 사용 인증 관리 기능

정책에 위반되거나 비 인가된 사용자에 대해서 IP 주소나 MAC 주소를 차단시킴으로써 네트워크 사용을 불가능하게 만들고 보안을 강화할 수 있음.

사용/미사용 IP 주소 관리

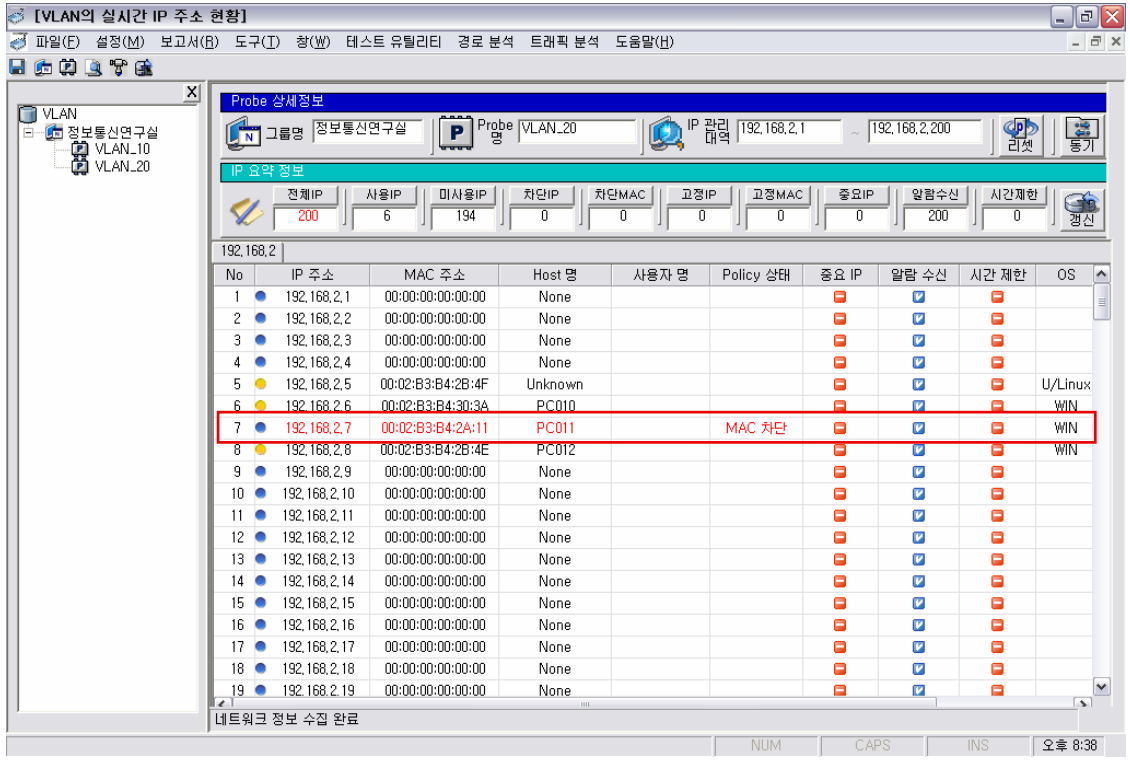
- 사용 중인 IP 주소와 미사용 중인 IP 주소를 구분하여 관리
- 네트워크 자원의 인증 여부를 확인 가능



(2) IP 주소 사용 인증 관리 기능

사용중인 IP 주소 관리

관리 시스템이 에이전트 시스템에게 IP 주소 차단, MAC 주소 차단의 명령을 수행시킴.



<MAC 주소 차단>

(3) 보고서 기능

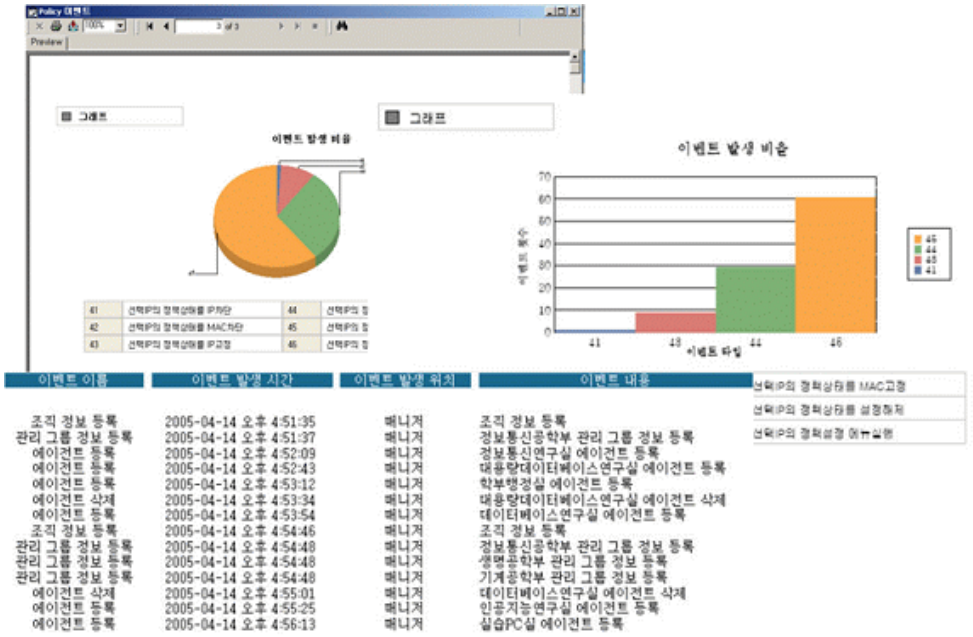
- 네트워크에서 수집된 모든 정보는 정형화된 보고서 형태로 볼 수 있는 기능
- 분석하는 요청자의 관점에 따라 크게 총괄 보고서와 세부 보고서로 구분

총괄 보고서

- 그룹별로 IP 주소 사용 내역에 대한 보고서를 관리자에게 제공
- 총괄 보고서를 바탕으로 개략적인 네트워크의 현 상태 및 장애에 대한 분석 가능

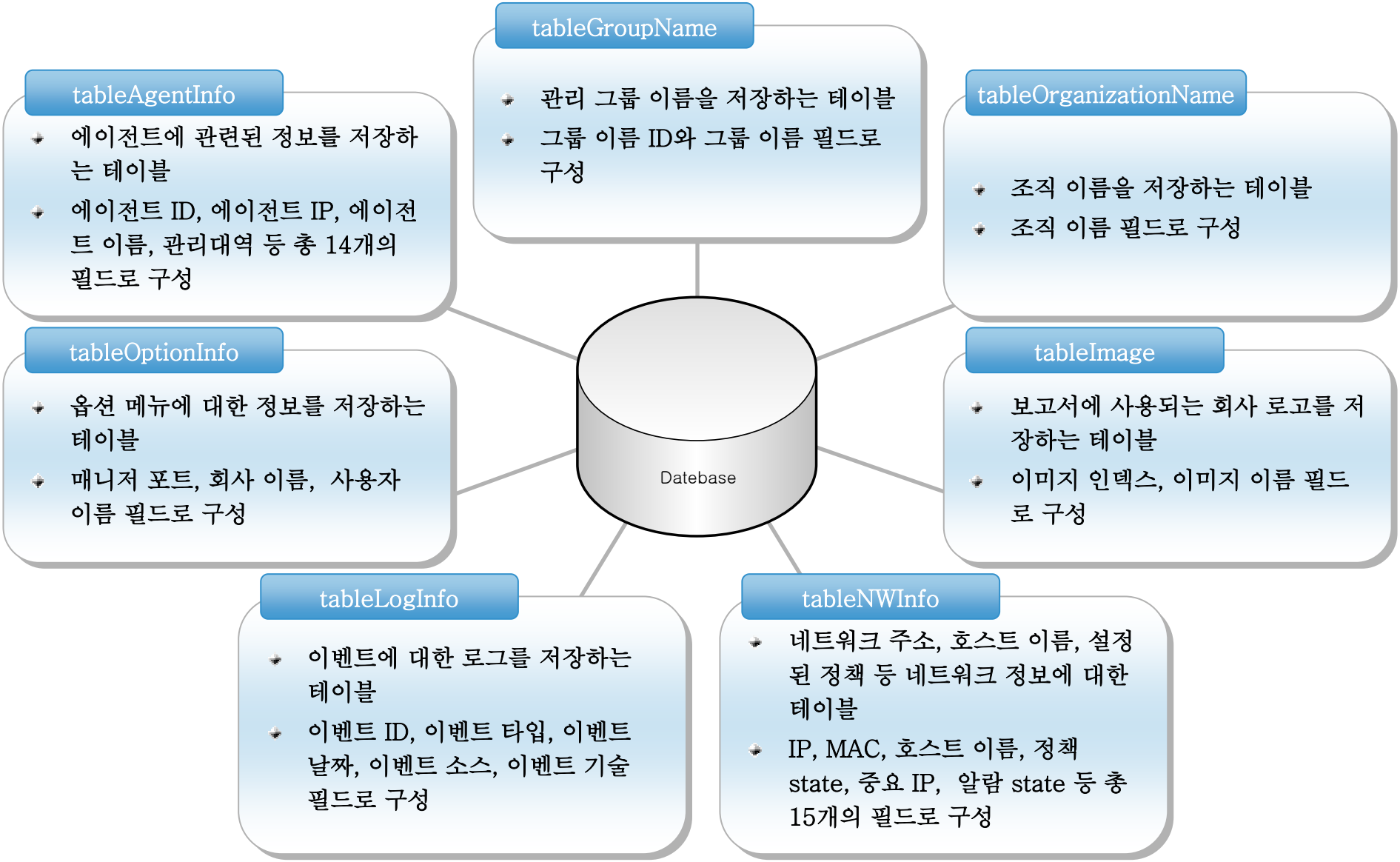
세부 보고서

- 로그파일에 대해 IP 주소별로 IP 주소 사용 내역에 대한 개별 보고서
- 네트워크 내의 관리 대상들에 대한 명확하고 직관적인 보고서들을 제공

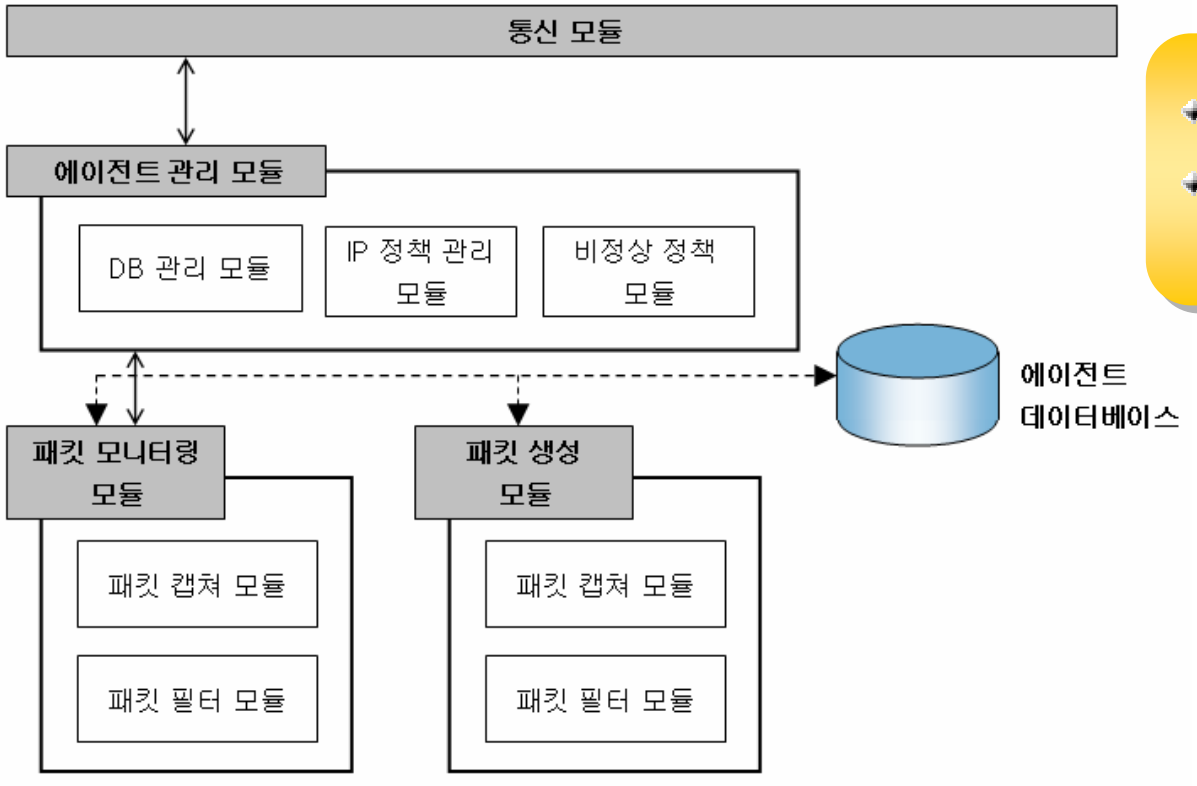


<보고서 기능>

Manager System - 8



Agent System - 1



- 각 모듈은 기능별로 모듈화
- 패킷 모니터링 모듈, 패킷 생성 모듈로 구성

Agent System - 2

- ARP 브로드캐스팅 도메인마다 설치
- 네트워크의 자원 정보 및 IP 주소를 수집하여 관리 시스템에게 통보
- 매니저 시스템의 정책에 따라 IP 주소 제어
- 중앙집중적인 관리 방식은 트래픽의 과부화 발생을 야기시키므로 분산적인 네트워크 환경에서 에이전트 개념을 적용시킨 시스템 개발이 필요

(1) 네트워크 자원 정보 자동 수집 기능

- 네트워크에 연결된 모든 자원인 IP 주소, MAC 주소, 시스템 이름, 사용자 이름을 자동으로 수집
- 수집된 정보는 매니저 시스템에게 전달
  - 매니저 시스템은 전달받은 정보로 현재 사용 중인 IP 주소 현황을 파악
  - 매니저 시스템은 필요에 따라 IP 차단과 같은 제어 기능 수행

Agent System - 3

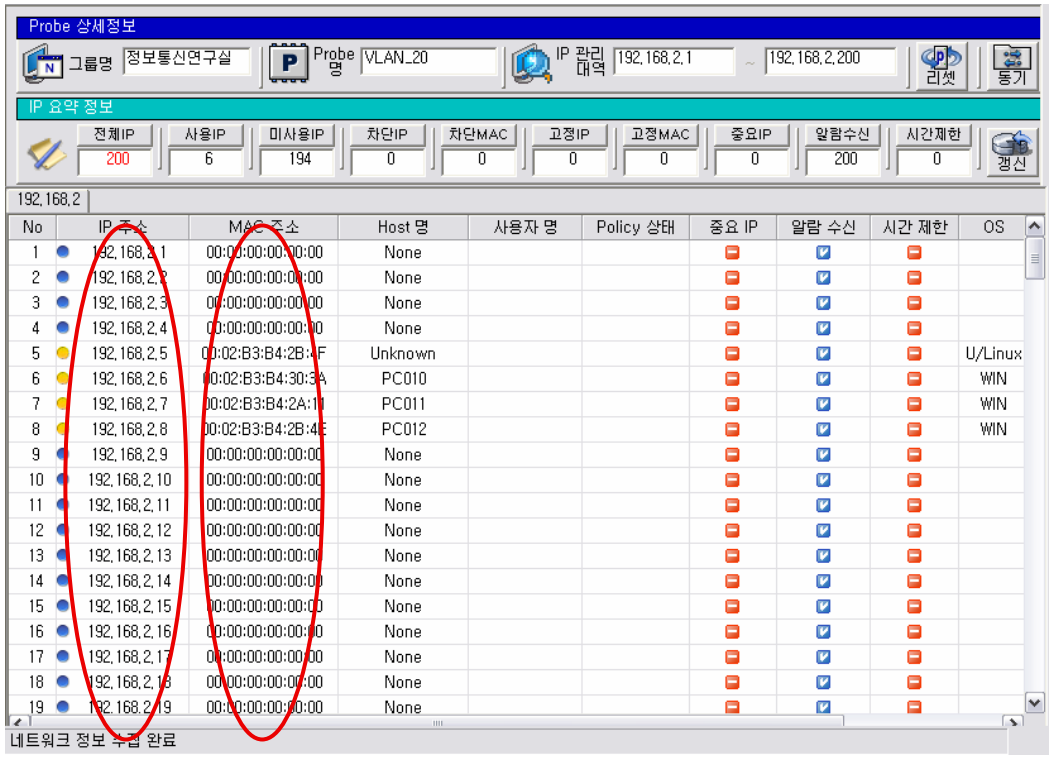
(1) 네트워크 자원 정보 자동 수집 기능

IP 주소

- 인터넷 상의 한 컴퓨터에서 다른 컴퓨터로 데이터를 보내는데 사용되는 프로토콜
- 각 호스트마다 고유한 주소를 할당
- IP 주소의 고유성은 보안 정책을 수행하는 데이터로 사용

MAC 주소

- 데이터 링크 계층의 MAC 계층에서 사용되는 고유한 주소
- 보안 정책을 수행하는 데이터로 사용



<네트워크 자원의 자동 수집 기능>

Agent System - 4

(2) 패킷 모니터링 기능

- 패킷 모니터링은 실시간으로 수행
- 수집된 데이터는 일정한 주기를 두고 매니저에게 전송되어 정책 반영에 영향
- 모니터링 모듈은 패킷이 ARP인 경우, 같은 네트워크에서 통신하는 IP인 경우, 특정 포트로 통신하는 TCP, UDP 패킷인 경우로 분리하여 패킷의 주소를 데이터베이스에 저장

로그파일 저장

- 사용자 별 실시간 특정 IP에 대해 MAC 및 사용자명 변경 여부를 체계적으로 관리하여 내부 보안 사고에 대한 추적 가능
- 사용자에서 발생된 실시간 이벤트 현황을 History화 하여 발생된 내부 문제점에 대해 빠른 조치가 가능

패킷 분석 및 데이터베이스 기록

패킷을 수집하고 분석하여 송신지와 수신지 IP 주소를 에이전트 시스템의 데이터베이스에 기록

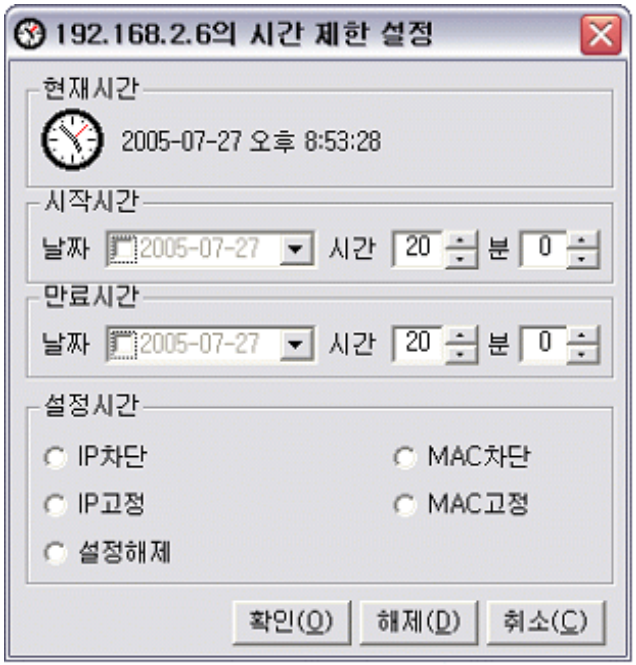
(2) 패킷 모니터링 기능

IP 주소 충돌 감지

- 사용자 별 실시간 특정 IP에 대해 MAC 및 사용자명 변경 여부를 체계적으로 관리하여 내부 보안 사고에 대한 추적 가능
- 사용자에서 발생된 실시간 이벤트 현황을 History화 하여 발생된 내부 문제점에 대해 빠른 조치가 가능

사용 기간 예약 및 제한

사용자 별 내부 직원 및 외부 방문 사용자에 대해 IP를 사용할 수 있는 기간을 예약 설정하여 기간이 만료된 사용자에 대한 효율적인 관리 가능



<사용 기간 예약 및 제한 설정>

(3) 패킷 생성 기능

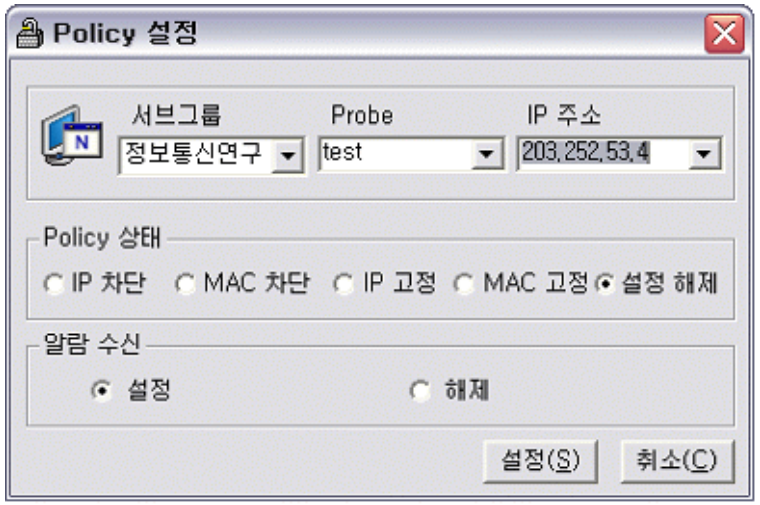
- 관리 시스템으로부터 인가된 IP 주소 목록을 전달받아 현재 네트워크에서 실시간 모니터링 기능으로 수집한 IP 주소를 비교하여 비 인가된 IP 주소가 사용 중이면 이 IP 주소를 차단
- ARP 패킷을 생성하여 차단 메커니즘을 수행

비 인증 IP 사용자 차단

- 관리자에 의해 인증되지 않은 사용자에 대해 차단을 하여 효율적인 IP 사용이 가능
- 부여된 IP에 대해 MAC 주소를 고정하여 보안성을 강조

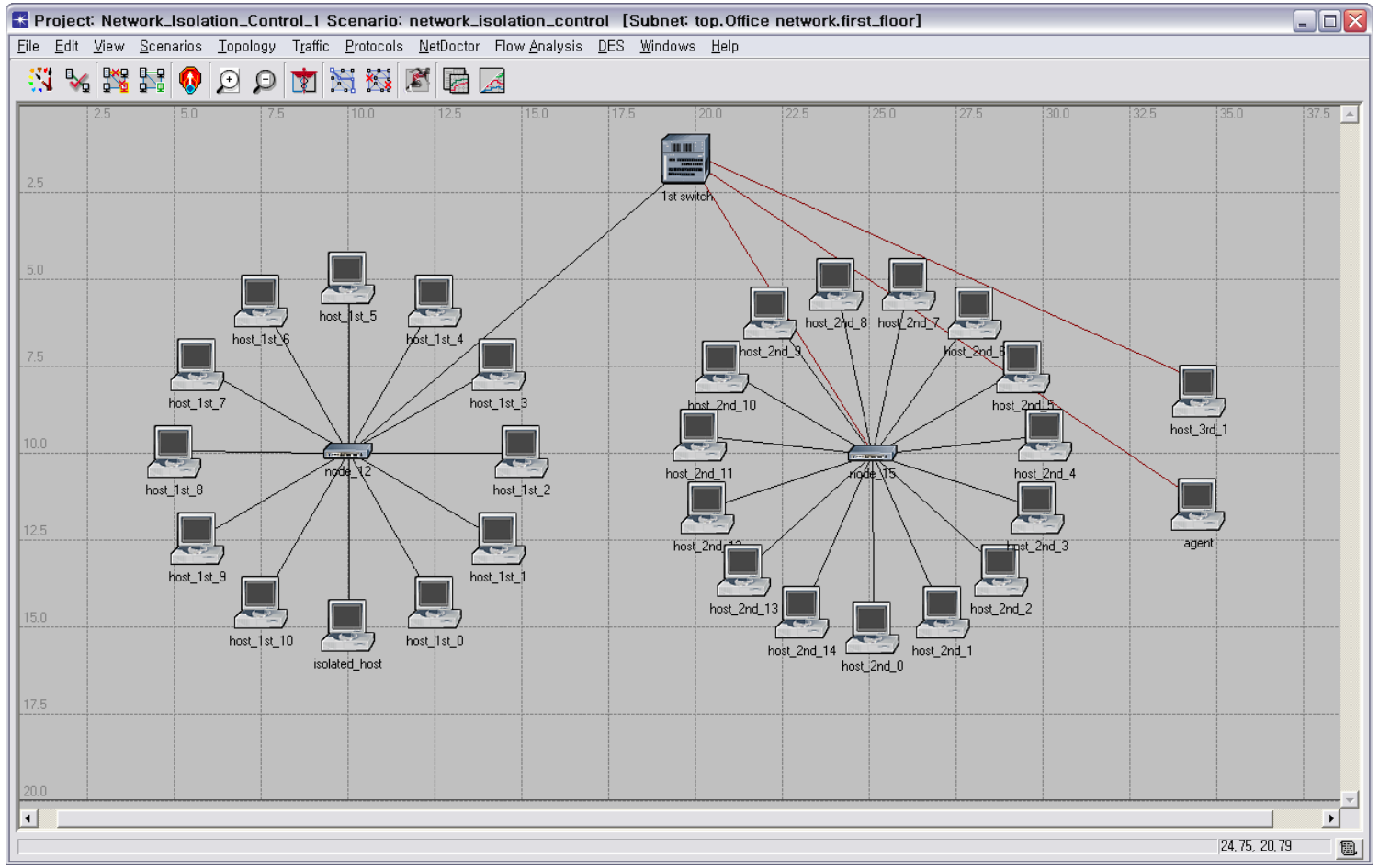
비 인증 MAC 사용자 차단

- 관리자에 의해 인증되지 않은 사용자에 대해 차단을 하여 효율적인 MAC 사용이 가능
- 부여된 MAC에 대해 IP 주소를 고정하여 보안성을 강조



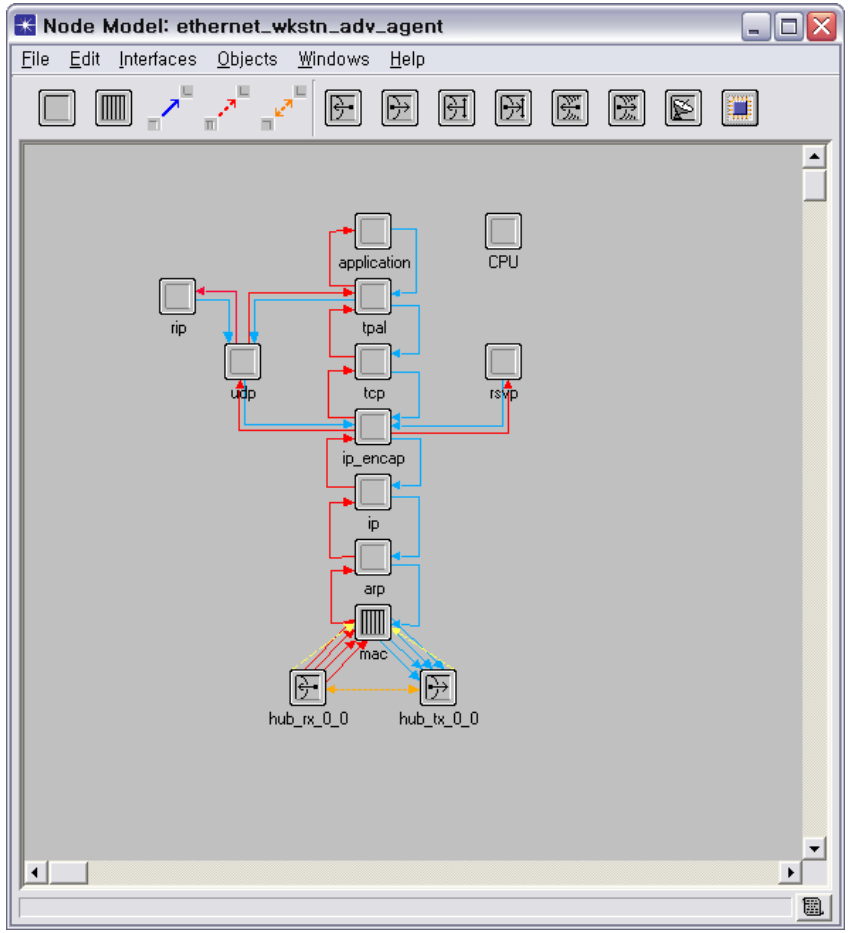
<Policy 설정>

Simulation - 1



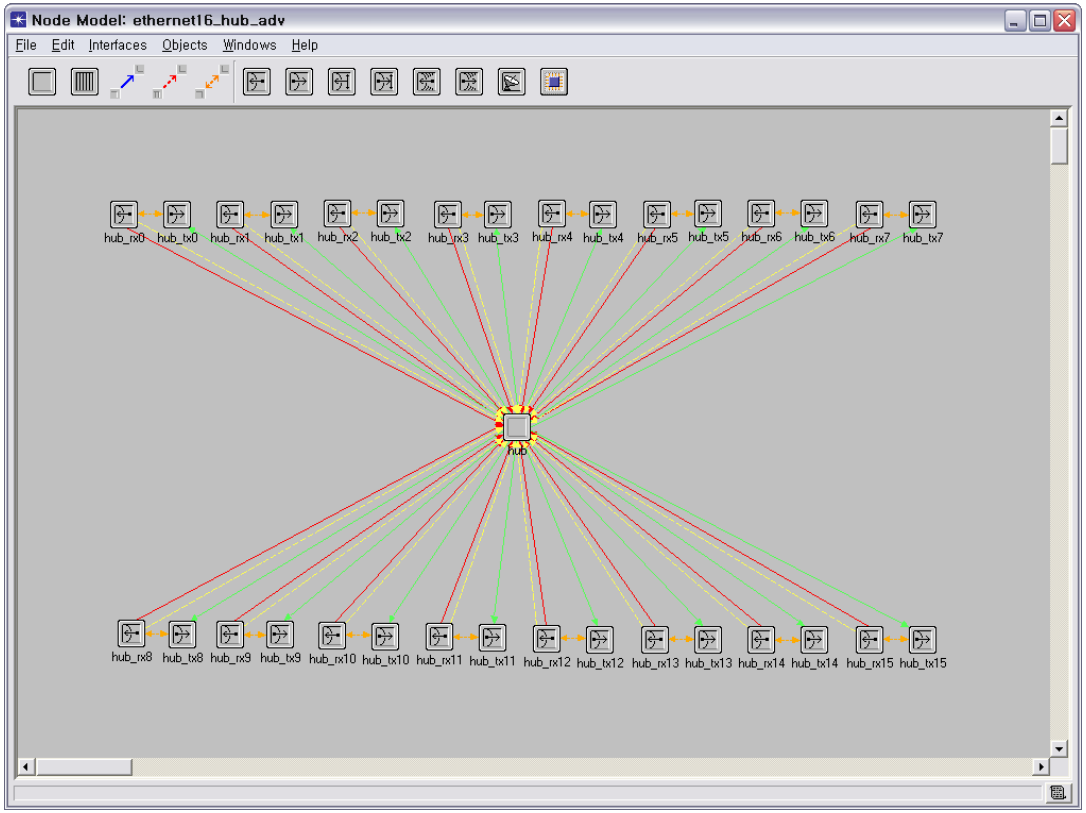
<정책 기반 실시간 네트워크 차단/통제 시스템의
네트워크 모델링>

Simulation - 2



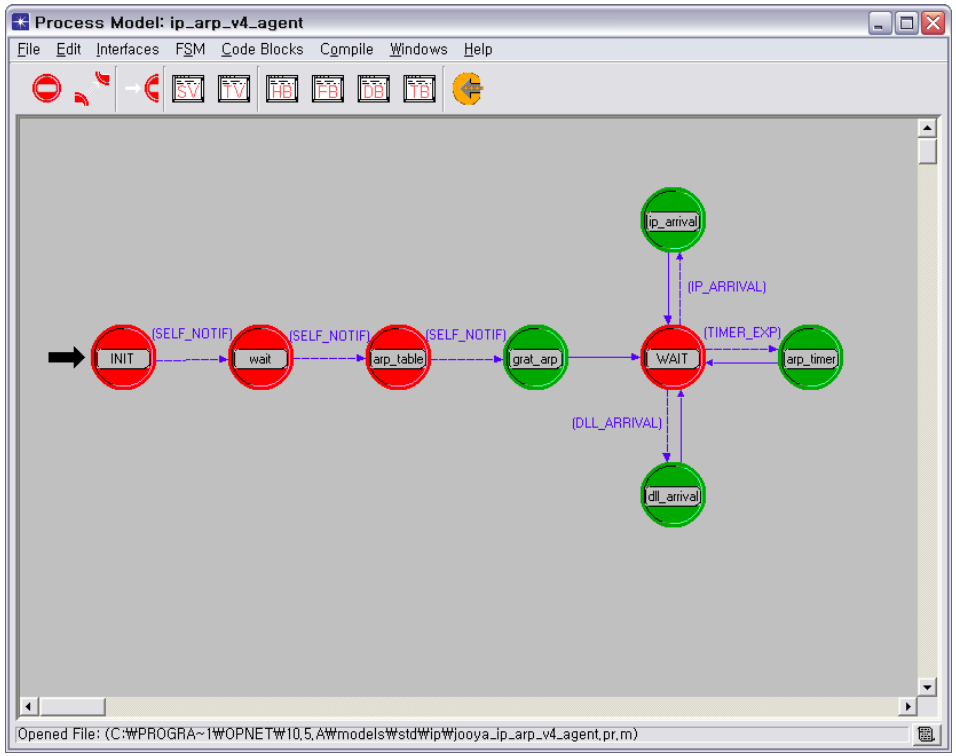
<정책 기반 실시간 네트워크 차단/통제 시스템
에이전트 모델링>

Simulation - 3



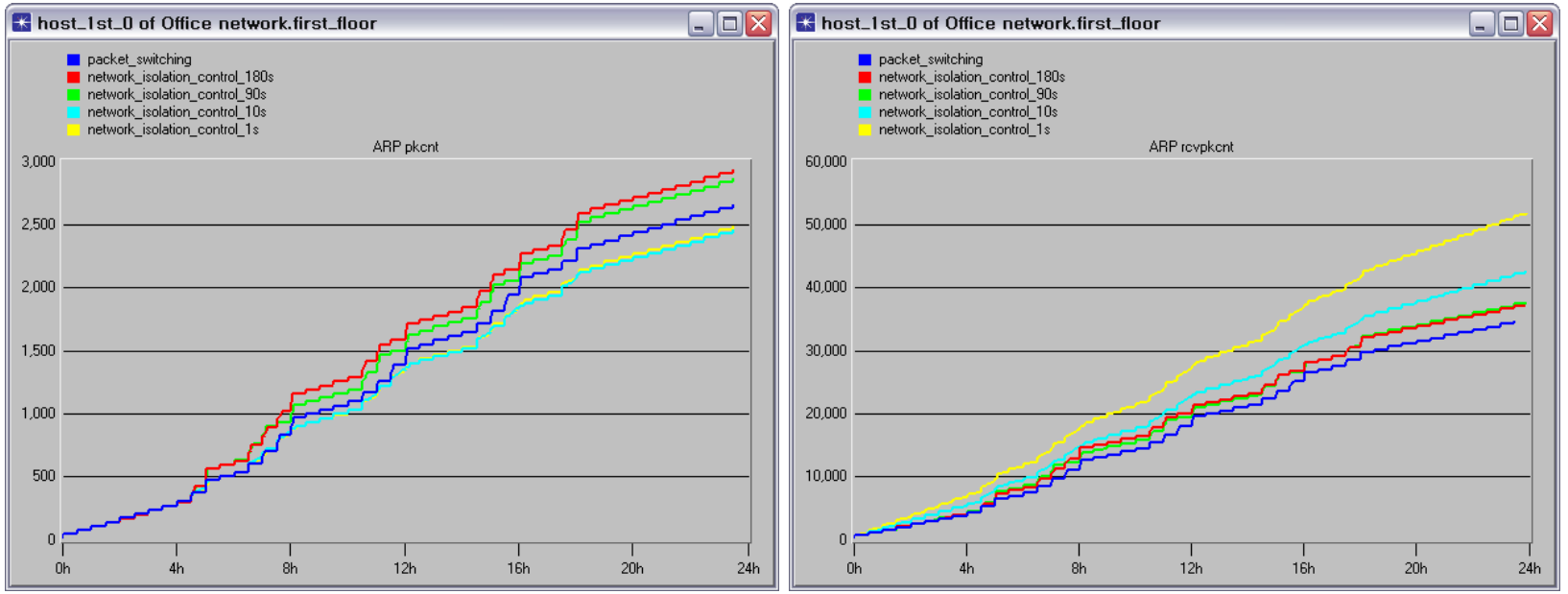
<실시간 네트워크 차단/통제 시스템 허브 노드 모델링>

Simulation - 4



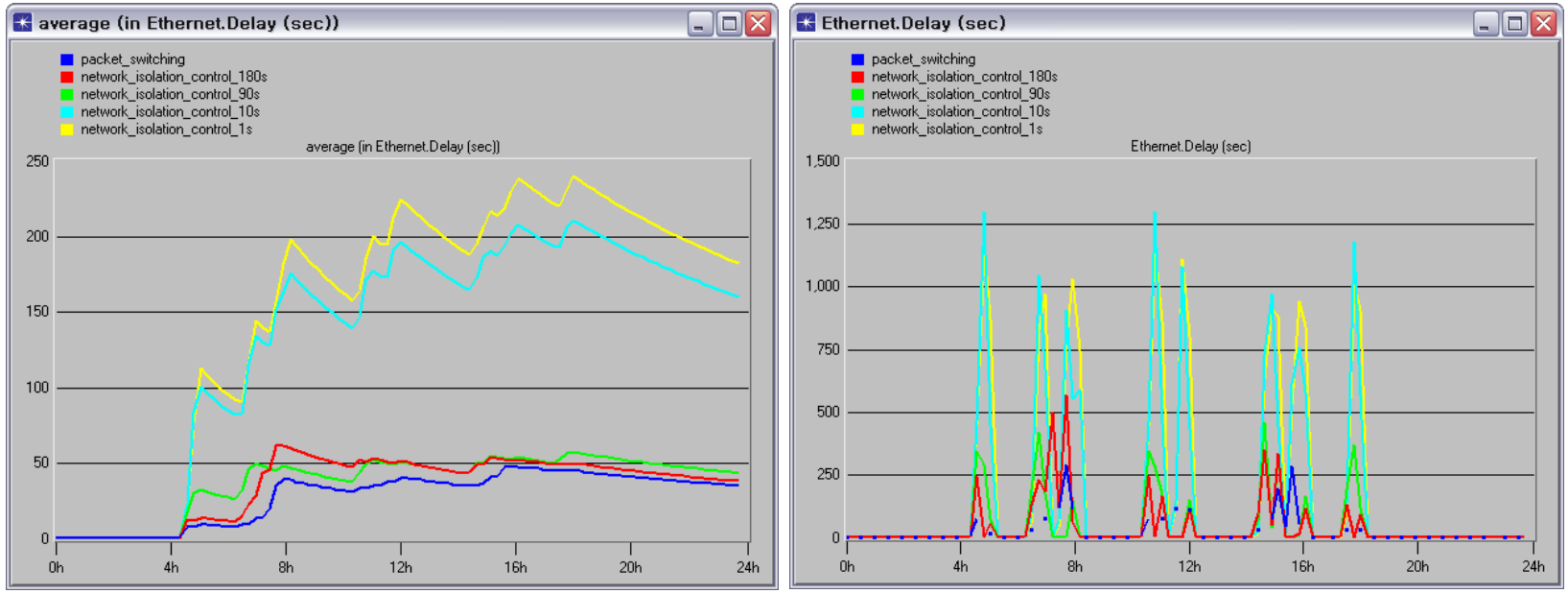
<arp 프로세스 모델링>

Simulation - 5



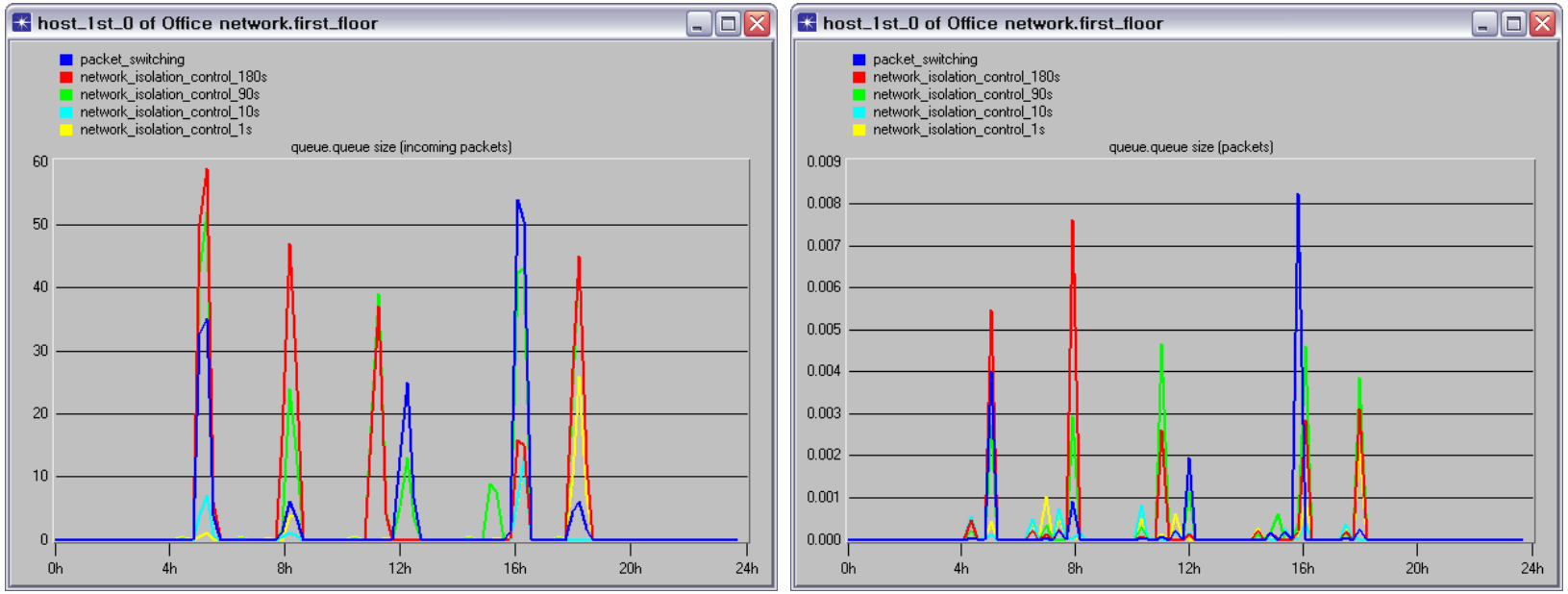
<arp Traffic>

Simulation - 6



<Ethernet Delay>

Simulation - 7



<Queue Size>

감사합니다.